Internal Audit Report

Computer Virus Detection
April 2003

Audit Team Members

Sandy Chockey, IT Consultant

Susan Adams, Senior IT Auditor

Maricopa County Internal Audit Department *“Do the right things right!”*

Maricopa County

Internal Audit Department

301 West Jefferson St
Suite 1090
Phx, AZ 85003-2143
Phone: 602-506-1585
Fax: 602-506-8957
www.maricopa.gov

April 29, 2003

Fulton Brock, Chairman, Board of Supervisors
Don Stapley, Supervisor, District II
Andrew Kunasek, Supervisor, District III
Max W. Wilson, Supervisor, District IV
Mary Rose Wilcox, Supervisor, District V

We have completed our review of the County's computer virus detection procedures. The audit was performed in accordance with the annual audit plan that was approved by the Board of Supervisors.

The highlights of this report include the following:

- Overall, the County anti-virus software procedures appear to be adequate to prevent and detect the existence or spread of computer viruses.
- Anti-virus software has not been installed on some County's web servers and laptop computers.
- County Policy does not include a centralized monitoring and reporting function that could enhance existing virus prevention efforts.

Attached are the report summary, detailed findings, recommendations, and management's response. We have reviewed this information with management and appreciate the excellent cooperation provided by management and staff. If you have questions, or wish to discuss items presented in this report, please contact Sandy Chockey at 506-1006.

Sincerely,

Ross L. Tate

Ross L. Tate
County Auditor

(Blank Page)

Table of Contents

Executive Summary

Centralized Monitoring (Page 6)

The County does not have a centralized monitoring and reporting function for computer virus detection and prevention. Downtime resulting from a virus infection can cost the County over $126,000 per hour. A centralized monitoring and reporting function could enhance existing virus prevention efforts and help enforce County policy. Centralization would also allow trending of data and could facilitate prompt identification and correction of any problem areas. The Office of the Chief Information Officer should review the feasibility of implementing a centralized virus monitoring and reporting function.

Public Health (Page 7)

While Public Health is using anti-virus software to protect the majority of its servers and desktops, anti-virus software has not been installed on its web servers and many of its laptop computers. If virus protection software is not used to detect and destroy viruses, the risk increases that viruses can be spread throughout the department and the County. Public Health should install anti-virus software on its web servers and laptop computers.

E-Government Technology (Page 8)

The County's major anti-virus server is managed and maintained by the E-Government group under the Chief Information Officer. As part of the multi-tiered virus protection program, guidelines have been established to provide a consistent practice for deploying and managing anti-virus software. Currently, over 40 County departments are supported by the E-Government server. We found that proper procedures and automated tools are used for handling, monitoring, updating, and administering virus protection on County computer systems.

Maricopa Integrated Health Systems (Page 9)

Maricopa Integrated Health System's (MIHS) anti-virus protection efforts appear to comply with County policy. Proper procedures and automated tools are used for handling, monitoring, updating, and administering virus protection on MIHS servers, personal computing devices, and operating and network systems. No exceptions or issues were noted.

Telecommunications (Page 10)

The Data Network device (or black box) which controls web access is another component of the network that requires anti-virus protection. The configuration of the black box appears to comply with County Policy. There were no exceptions noted. Proper procedures and automated tools are used for handling, monitoring, updating, and administering virus protection on the black box.

Introduction

Background

A computer virus is code that has been purposely written to cause damage to software or data files, or to attempt to 'hijack' a computer. Viruses execute on a specified trigger, such as running a program, opening an email, or visiting a specific website. Viruses can inflict damage from deleting files to rendering a computer unusable.

Computer viruses continue to increase at an unprecedented rate. Over 70,000 viruses are known to exist with approximately 1,200 new viruses discovered every month. During the last year, instances of email viruses have doubled from one in every 400 emails to one in every 200 emails. Computer Economics, a technology consulting company, reports that new strains of computer viruses caused billions of dollars in damage in 2001, due to network crashes and related costs. Because viruses can have such devastating effects, it is vital that industry best practices are implemented to guard against infection.

Industry Best Practices

Industry best practices related to virus detection and prevention include:

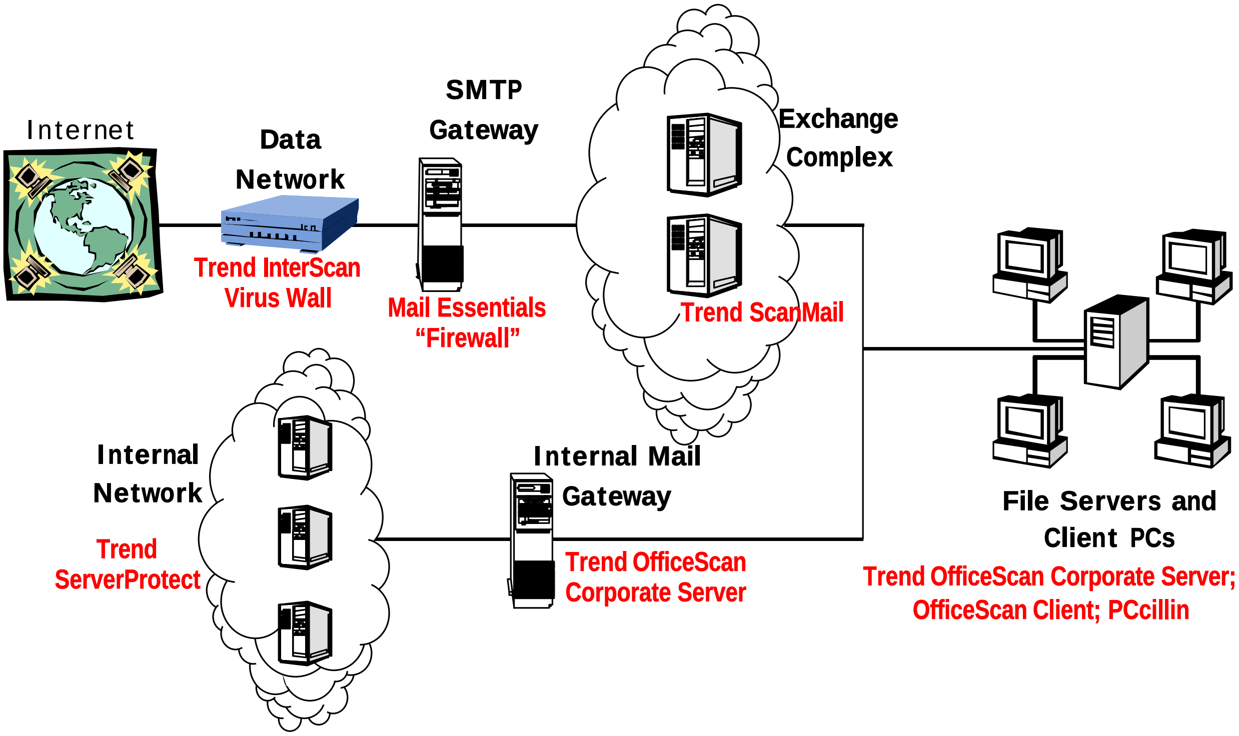
- Using the most current anti-virus software and virus definitions
- Scanning all incoming and outgoing files, disks, email attachments, and executable files
- Ensuring the software and definitions are used on all firewalls, file servers, application servers, and workstations

Anti-virus software should be incorporated into the firewall to detect and prevent viruses from entering the computer network. Anti-virus software should be loaded on all file servers and workstations to protect against any virus that may penetrate the firewall.

County Virus Protection Efforts

Maricopa County is vulnerable to several virus propagation possibilities. Viruses can be received from the Internet through inbound email as well as downloaded files. Viruses can also be introduced into the County network through floppy, zip disk, or remote access. To protect against these vulnerabilities, the County has established a multi-tiered virus protection program. The County has contracted with Trend Micro Systems and uses the Trend anti-virus software suite for virus detection and protection. The diagram on the next page shows the current levels of anti-virus software. The Trend software products are indicated in red.

Multi-Tiered Virus Protection System



Internet
Data Network
Trend InterScan Virus Wall
SMTP Gateway
Mail Essentials "Firewall"
Exchange Complex
Trend ScanMail
File Servers and Client PCs
Trend OfficeScan Corporate Server; OfficeScan Client; PCcillin
Internal Network
Trend ServerProtect
Internal Mail Gateway
Trend OfficeScan Corporate Server

The Data Network is the County's first level of defense prior to email reaching the exchange servers. Trend InterScan scans all simple mail transfer protocol (SMTP) traffic and automatically deletes an email message if a virus is identified.

Mail Essentials Firewall and Trend ScanMail scans mail messages and attachments for known email vulnerabilities. These messages are quarantined and a notification is sent to the designated recipient. If the designated recipient requests the message, it is manually scanned, cleaned (if necessary), and released to the recipient.

Trend ServerProtect scans application and file servers for viruses. Trend OfficeScan and PCcillin scans desktops and laptops for viruses.

As part of the multi-tiered virus protection program, the County has established guidelines to provide a consistent practice for deploying and managing anti-virus software. E-Government Technology, a group within the Office of the Chief Information Officer (OCIO), manages the Enterprise Solutions server for those departments who do not maintain their own OfficeScan Server. Currently, over 40 departments are supported by this server. Departments not supported by the server are responsible for their own anti-virus protection.

Scope and Methodology

The scope of the audit included a review of departments supported by the Enterprise Solutions Server managed by OCIO, departments that administer their own virus protection program, and the Data Network (black box), which is managed and maintained by the Telecommunications Department.

The objectives of this audit were to determine if:

- The County has developed and implemented policies and procedures that accurately reflect the intentions of management and lend themselves to thorough protection of computer systems from virus infections.
- Information housed on the network is safeguarded by current virus protection software.
- Virus protection is comprehensive and maintained on all necessary equipment.
- Virus protection software scans are appropriately scheduled.

This audit was performed in accordance with generally accepted government auditing standards.

Department Reported Accomplishments

The Chief Information Officer has provided the Internal Audit Department with the following information for inclusion in this report.

Anti-Virus Strategy – Software Solutions

Strategies have been developed through the PC/LAN community of interest. A special subcommittee comprised of technical specialists within the county has developed a multi-layered virus defense approach. The “Trend Micro” anti-virus software suite selection was approved by the PC/LAN community and enterprise pricing was negotiated at a cost savings of over $150,000 in May of 2001.

Virus Policy

A formal policy addressing virus protection was developed and subsequently published in April of 2001.

MfR Statistics

Quarterly, all PC/LAN managers report the number of active PCs and servers registered in their Trend anti-virus database. This number is matched against the number of licenses purchased by the department to determine if any systems may be lagging behind in their use of anti-virus software.

Vulnerability Audits & Security Alerts To PC/LAN Managers

For nearly five years the County has had a program in place for Internet connected servers that ensures they are audited for security vulnerabilities. Additionally, these servers are frequently scanned using tools that a hacker might employ to further test how well secured they are.

Virus Response Plan & Team

A virus “SWAT” team was formed in 2001 to organize the communication and technical collaboration of technologists in the event of a virus outbreak. This team has a defined mode of communication, time intervals in which they meet and there is continuous effort in fine-tuning the processes used in the event of an outbreak.

Enterprise Level Coordinator

The County Network Security Officer will provide coordination for the County’s network vulnerability and virus protection program. This enterprise level coordination will include collaboration with all County Departments and IT support teams to implement, manage, and provide ongoing evaluation of the effectiveness of the County’s multi-layered virus defense approach.

Investigate And Evaluate Video Opportunity

A kick-off meeting with the video team is scheduled for late February. The purpose of the video will be to educate the end-user community regarding the topic of computer viruses.

Develop “Tips And Tricks” Brochure For All Active Card Users

Telecom is creating a small brochure with tips for telecommuters and vendors who have access into our systems on security related issues. Included will be information warning these end-users about security risks and advise them on how to best secure their remote PC so we minimize the chance they’ll present a security breach into our network.

Issue 1 Centralized Monitoring

Summary

The County does not have a centralized monitoring and reporting function for computer virus detection and prevention. Downtime resulting from a virus infection can cost the County over $126,000 per hour. A centralized monitoring and reporting function could enhance existing virus prevention efforts and help enforce County policy. Centralization would also allow trending of data and could facilitate prompt identification and correction of any problem areas. The Office of the Chief Information Officer (OCIO) should review the feasibility of implementing a centralized virus monitoring and reporting function.

Enterprise-Wide Policy

County policy A1610 was created to help “eliminate insidious infections and avoid severe service disruptions for County departments.” In addition, the County’s PC/LAN managers created the *Anti-Virus Guidelines and Information* document to provide “best-practices” for implementing and administering virus protection within the County. However, neither the policy nor the guidelines address any type of centralized monitoring function.

Risk

Lack of adequate virus protection policies and procedures could result in downtime, and may have a substantial impact on the County. For example, the County’s average wage is $18.05 per hour, given 14,000 employees, the County could lose $252,700 for every hour its employees cannot use their computers. Assuming a more conservative estimate that employees use their computers only 50 per cent of the time, down-time due to a computer virus could cost the County $126,350 per hour. This does not take into consideration the additional cost associated with researching the problem, bringing the systems back on-line, and purging the virus.

Centralizing the virus monitoring function would help ensure the enforcement of County policy relating to anti-virus efforts. Centralized monitoring would help ensure that software deployment, information on current engines, and signature files are consistently communicated and applied throughout the County. A centralized reporting function would also allow Countywide statistics to be compiled, monitored, and analyzed to determine the effectiveness of the County’s virus detection efforts. Data trends revealing potential problem areas could be isolated and flagged for further review.

Recommendation

The OCIO should:

A. Consider implementing a centralized monitoring and reporting function for computer virus detection.

B. If appropriate, establish procedures related to a centralized reporting function including, but not limited to, information that is to be monitored and reported, whom the information will be reported to, and the types of analysis that will be performed.

Issue 2 Public Health

Summary

While Public Health is using Trend anti-virus software to protect the majority of its servers and desktops, anti-virus software has not been installed on its Apple web servers and many of its laptop computers. If virus protection software is not used to detect and destroy viruses, the risk increases that viruses can be spread throughout the department and the County. Public Health should install anti-virus software on its Apple web servers and laptop computers.

Policy Requirements

County policy A1610 states that each department is responsible to "install and maintain anti-virus programs for the prevention of infection and/or infected systems…. All county departments shall take due diligence in implementing and maintaining anti-virus programs (software) on servers, personal computing devices, and operating, network, and communication systems."

Risks

Public Health is currently using the Trend anti-virus software to protect most of its servers and desktops. Based on our review, current software configurations are in compliance with established County guidelines. This includes software installation, software updates, and monitoring of computer viruses.

However, we found that Public Health had not installed anti-virus software on its Apple web servers. Trend Micro, the County's anti-virus software vendor, does not have a product that protects the Apple web servers. Public Health is relying on updating software patches for its operating system as a way of protecting the servers. Public Health has considered a different virus software vendor but some questions arose as to the effectiveness of their product. Public Health has not yet researched other alternatives. If virus protection software is not used to detect and destroy viruses, the risk increases that viruses can be spread throughout the department and the County.

Furthermore, Public Health has not installed anti-virus software on all of its laptop computers. The laptops do not connect to the network and can not perpetuate a virus on the network. However, the work performed using the laptop computers may be in jeopardy without adequate anti-virus protection.

Recommendation

Public Health should install anti-virus software on its Apple web servers and its laptop computers to ensure complete virus protection of County servers and personal computing devices.

Issue 3 E-Government Technology

Summary

The County's Enterprise Solutions server is managed and maintained by the E-Government (E-Gov) group under the Chief Information Officer. As part of the multi-tiered virus protection program, guidelines have been established to provide a consistent practice for deploying and managing anti-virus software. Currently, over 40 County departments are supported by the Enterprise Solutions server. We found that proper procedures and automated tools are used for handling, monitoring, updating, and administering virus protection on County computer systems.

County Policy

Maricopa County Policy A1610 states that each department is responsible to "install and maintain anti-virus programs for the prevention of infection and/or infected systems." The County PC/LAN managers have also adopted the *Anti-Virus Guidelines and Information* document which provides guidelines and information for use in deploying, updating, and managing anti-virus software within County departments. The guidelines establish Trend anti-virus software as the standard to be used by all departments and agencies throughout the County.

Best Practice

E-Gov is responsible for managing the Enterprise Solutions server which provides virus detection and protection for departments supported by E-Gov, as well as other departments that have elected to have E-Gov manage their virus protection program. Currently, over 40 departments are supported by the anti-virus programs located on the Enterprise Solutions server.

E-Gov has installed the Trend anti-virus software configuration as outlined in *the Anti-Virus Guidelines and Information* document. One exception is the updating of virus pattern files on an hourly basis. E-Gov found that updating the information each hour slowed their system performance to the point that it was unproductive for the users. Changing the updates to be less frequent allowed E-Gov to keep its virus definition files up to date on a reasonable basis but did not interfere with the work of the users. Furthermore, when Trend (vendor) releases an "emergency" update, E-Gov is immediately notified and the update is manually installed. E-Gov is also responsible for notifying the rest of the County PC/LAN groups of the new update.

Recommendation

None, for information only. E-Gov has adequate virus protection controls in place to protect its information systems.

Issue 4 MIHS

Summary

Maricopa Integrated Health System's (MIHS) anti-virus protection efforts appear to comply with County policy. Proper procedures and automated tools are used for handling, monitoring, updating, and administering virus protection on MIHS servers, personal computing devices, and operating and network systems. No exceptions or issues were noted.

Policy Requirements

Maricopa County Policy A1610 states that each department is responsible to "install and maintain anti-virus programs for the prevention of infection and/or infected systems." The County PC/LAN managers have also adopted the *Anti-Virus Guidelines and Information* document which provides guidelines and information for use in deploying, updating, and managing anti-virus software within County departments. The guidelines establish Trend anti-virus software as the standard to be used by County departments and agencies.

Best Practice

MIHS has installed Trend anti-virus software configuration as outlined in the *Anti-Virus Guidelines and Information* document. One exception is updating of virus pattern files on an hourly basis. MIHS found that updating the information each hour slowed their system to the point that it was unproductive for the users. Changing the updates to be less frequent allowed MIHS to keep its virus definition files up-to-date on a reasonable basis but did not interfere with the work of the users. Furthermore, if Trend (vendor) releases an "emergency" update, the system administrators are immediately notified and the update is manually installed.

Recommendation

None, for information only. MIHS has adequate virus protection controls in place to protect its information systems.

Issue 5 Telecommunications

Summary

The Data Network device (black box) which controls web access is another component of the network that requires anti-virus protection. The configuration of the black box appears to comply with County Policy. There were no exceptions to report. Proper procedures and automated tools are used for handling, monitoring, updating, and administering virus protection on the Data Network device.

County Requirements

Maricopa County Policy A1610 states that each department is responsible to “install and maintain anti-virus programs for the prevention of infection and/or infected systems.” Because the black box is the County’s first line of defense against viruses, it is critical that virus detection software updates and virus scanning procedures are properly managed.

Best Practice

The Telecommunications Department (Telecom) is responsible for maintaining the black box. Telecom is using Trend InterScan VirusWall software to detect viruses coming through the black box. Telecom has programmed its Trend anti-virus configuration to ensure that virus pattern files are updated regularly. If an emergency update is required, Telecom is notified directly by Trend (vendor) and they manually update the virus pattern file immediately.

Recommendation

None, for information only. Telecom has adequate virus detection controls over its black box.

(Blank Page)

Department Response

AUDIT RESPONSE
OFFICE OF THE CIO
COMPUTER VIRUS DETECTION APRIL 2003

Issue #1:
Centralized Monitoring

Response: Concur.

Recommendation A: The OCIO should consider implementing a centralized monitoring and reporting function for computer virus detection.

Response: Concur. The enterprise level coordinator (Chief Information Security Officer) will coordinate the defense and counter measures under the network protection umbrella. The CISO will evaluate the effectiveness of a multi-tiered defense through coordination with the PC/LAN managers. This coordination effort will be compatible/consistent with the federated governance model of the decentralized IT departments within the County.

Target Completion Date: 9/30/03

Benefits/Costs: Improved security and protection of County network and other computing assets.

Recommendation B: The OCIO should if appropriate, establish procedures related to a centralized reporting function including, but not limited to, information that is to be monitored and reported, whom the information will be reported to, and the types of analysis that will be performed

Response: Concur. The Chief Information Security Officer will work with the PC/LAN community to establish procedures and review the proposed procedures with the County CIO.

Target Completion Date: 9/30/03

Benefits/Costs: Improved security and protection of County network and other computing assets.

Approved By :

	Department Head/Elected Official	4/13/03 **Date**
	Chief Officer	4/13/03 **Date**
	County Administrative Officer	4/17/03 **Date**

Maricopa County

Department of Public Health

1845 East Roosevelt Street
Phoenix, Arizona 85006
Phone: (602) 506-6900
Fax: (602) 506-6885

TO: Ross L. Tate, County Auditor

FROM: Cedric Johnson, I.T. Director

DATE: March 21, 2003

SUBJECT: **COMPUTER VIRUS DETECTION DRAFT REPORT**

Pursuant to published Administrative Response Procedures, the Department of Public Health responds to the single issue raised by the audit, identified as Issue two (2).

Issue #2: Public Health should install anti-virus software on its Apple Web Servers, and on all Laptop Computers.

Response: Concur. The Department of Public Health has ordered a version of Norton Antivirus software for the Macintosh OS X environment. This software will be installed as soon as it arrives.

With regard to department laptop computers, the Information Technology Division will conduct a laptop update event, May 27th and 28th and require staff to bring in all laptop computers for inventory, and installation of Trend Virus Software. The majority of the departments laptop computers are not configured for network access (they lack both network clients, and IP addresses), therefore, virus installation and updates are manual. Additionally, most of these laptops are assigned to individual users, and for the most part are not utilized in the work environment for routine task. Department desktop units are not ordered with Floppy Disk Drives eliminating what was once the most common vector for virus infection between computer units.

Approved By: 4/17/03

Department Head\Elected Official Date

4/17/03

County Administrative Officer Date